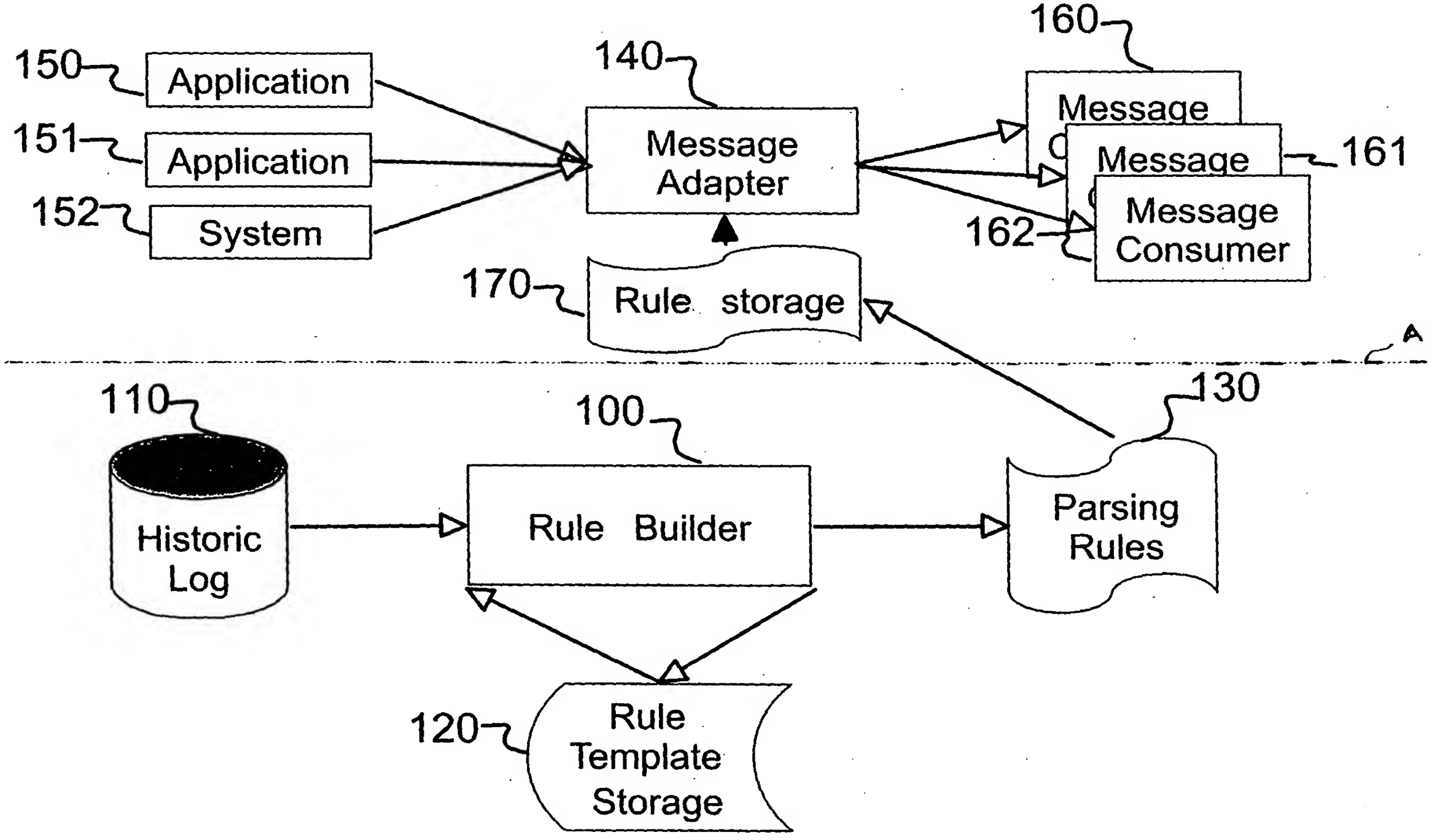
FIG.1



G. GRABARNIK ET AL.
10/720030326US1 (GRT2)

FIG. 2

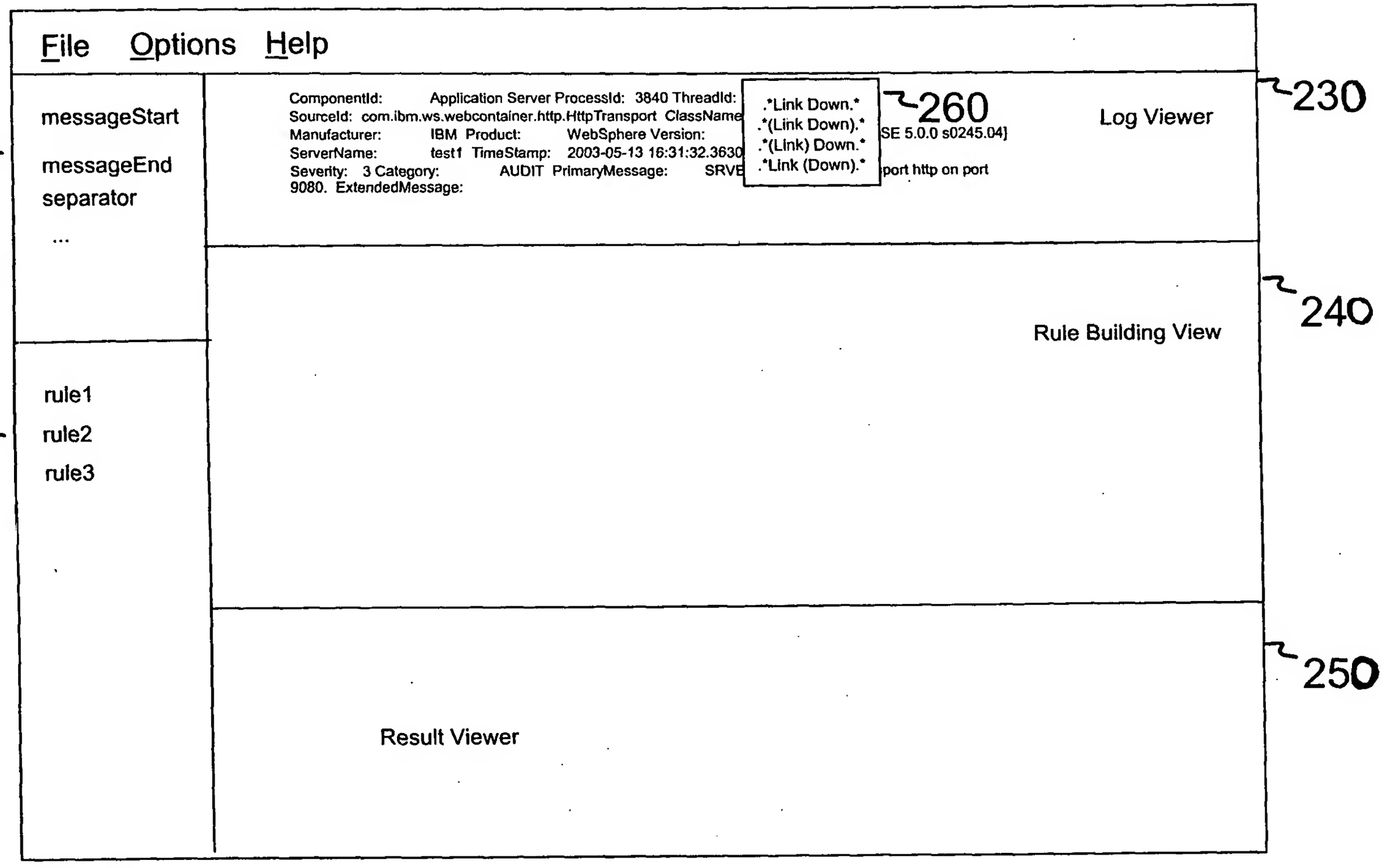

File Options Help
210
messageStart
messageEnd
separator
...
ComponentId: Application Server ProcessId: 3840 ThreadId:
SourceId: com.ibm.ws.webcontainer.http.HttpTransport ClassName
Manufacturer: IBM Product: WebSphere Version:
ServerName: test1 TimeStamp: 2003-05-13 16:31:32.3630
Severity: 3 Category: AUDIT PrimaryMessage: SRVE
9080. ExtendedMessage:
.*Link Down.*
.*(Link Down).*
.*(Link) Down.*
.*Link (Down).*
260
SE 5.0.0 s0245.04]
port http on port
Log Viewer
230
240
Rule Building View
220
rule1
rule2
rule3
250
Result Viewer

FIG.3

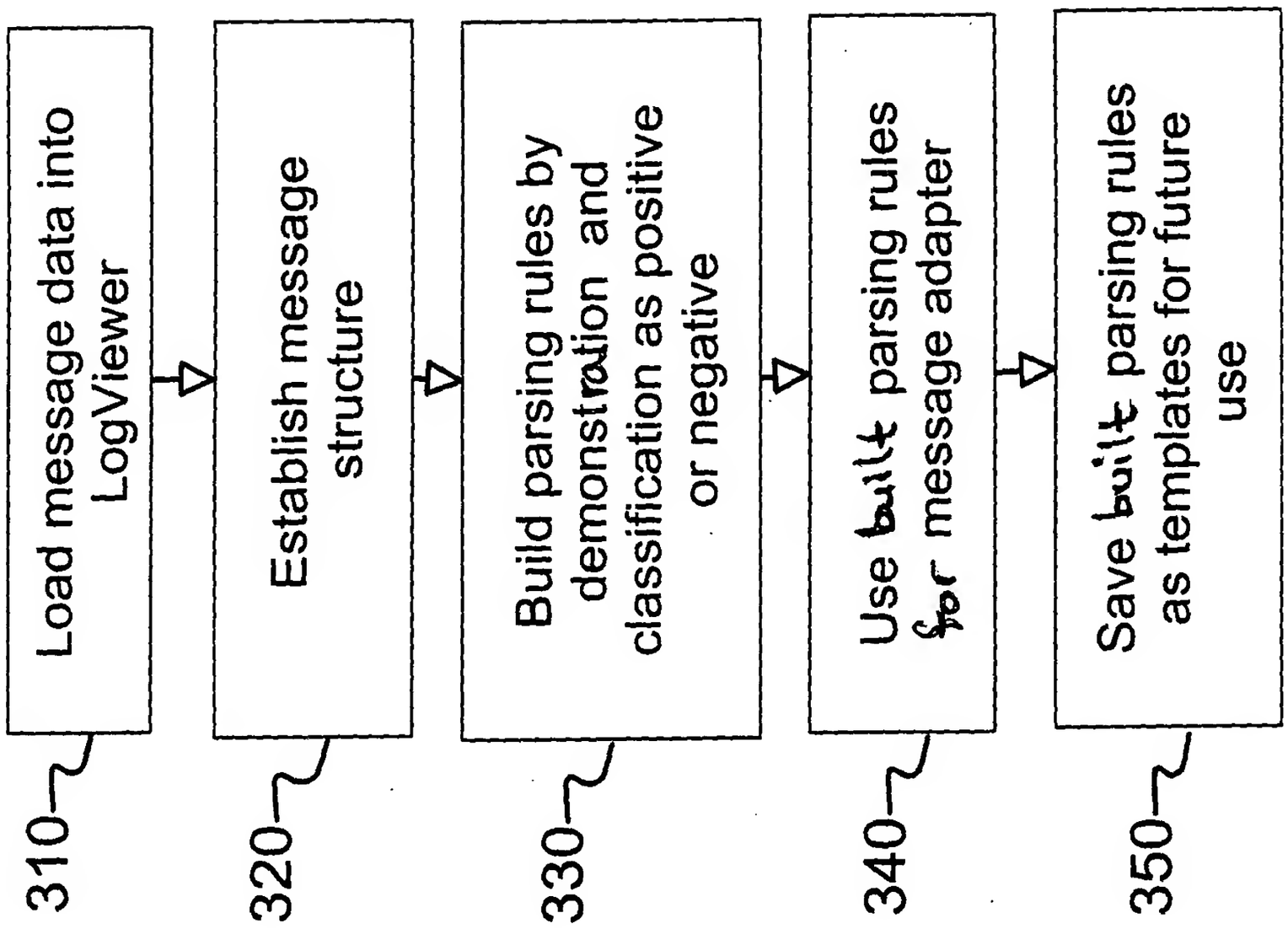

Load message data into LogViewer
310
Establish message structure
320
Build parsing rules by demonstration and classification as positive or negative
330
Use built parsing rules for message adapter
340
Save built parsing rules as templates for future use
350

FIG.4

400

```
<?xml version="1.0" encoding="UTF-8" ?>
<schema targetNamespace="http://MsgStructure.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
        <element name="MsgStructure">
                <complexType>
                        <attribute name="multiline" type="boolean"
default="false"/>
                        <attribute name="eventStart" type="string"/>
                        <attribute name="eventEnd" type="string"/>
                        <attribute name="separator" type="string" default="\s+"/>
                        <attribute name="msgType" type="MsgTypeType"/>
                        <attribute name="glueing" type="string" default=";"/>
                        <attribute name="matchContinue" type="string"/>
                </complexType>
        </element>
        <simpleType name="MsgTypeType">
                <restriction base="NCName">
                        <enumeration value="TEC_RECEPTION_MSG" />
                        <enumeration value="DB2_MSG" />
                        <enumeration value="WAS_ACTIVITY_LOG" />
                        <enumeration value="WAS_MSG" />
                        <enumeration value="UNKNOWN_MSG" />
                </restriction>
        </simpleType>
</schema>
```


4082003026US1

FIG.5

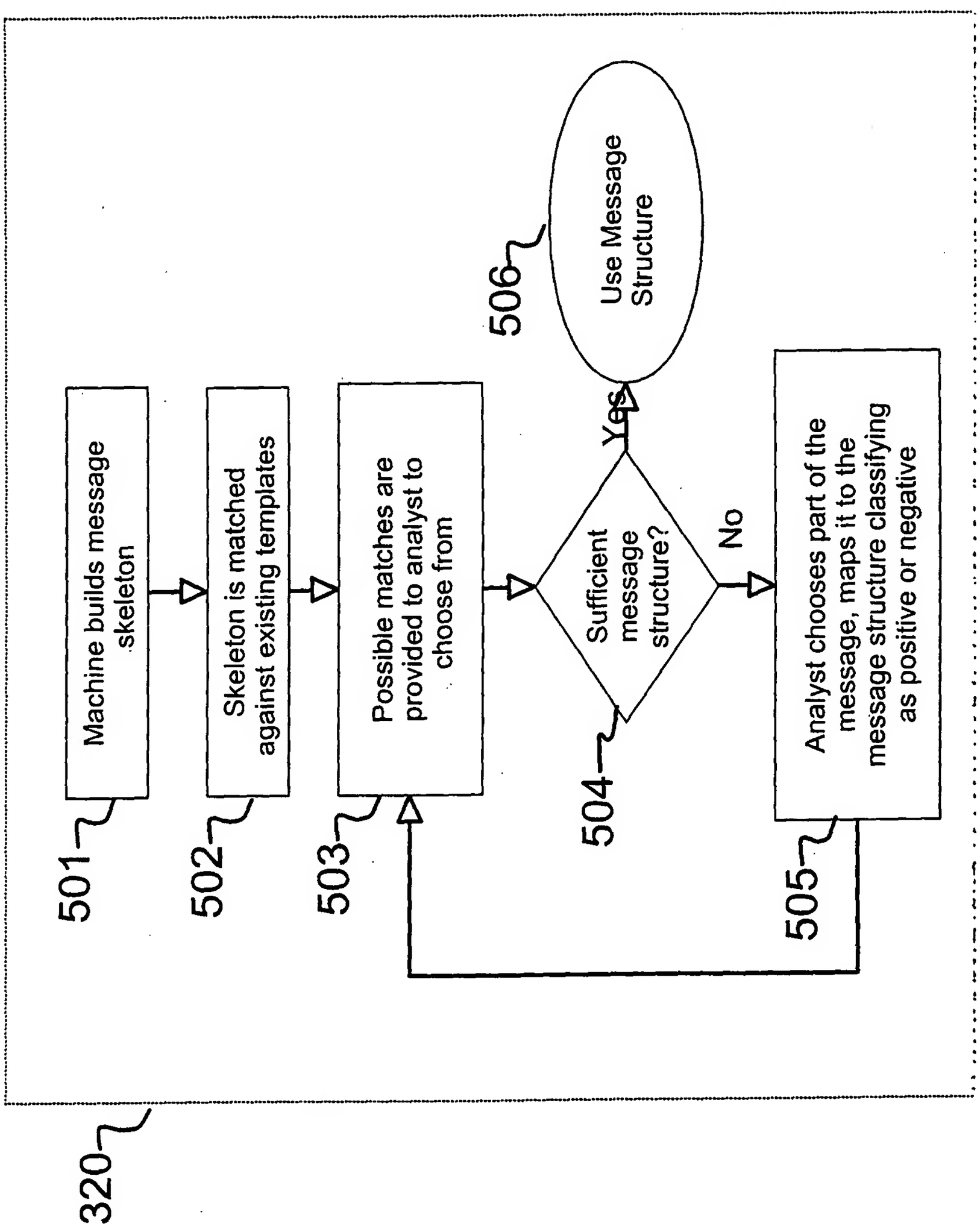
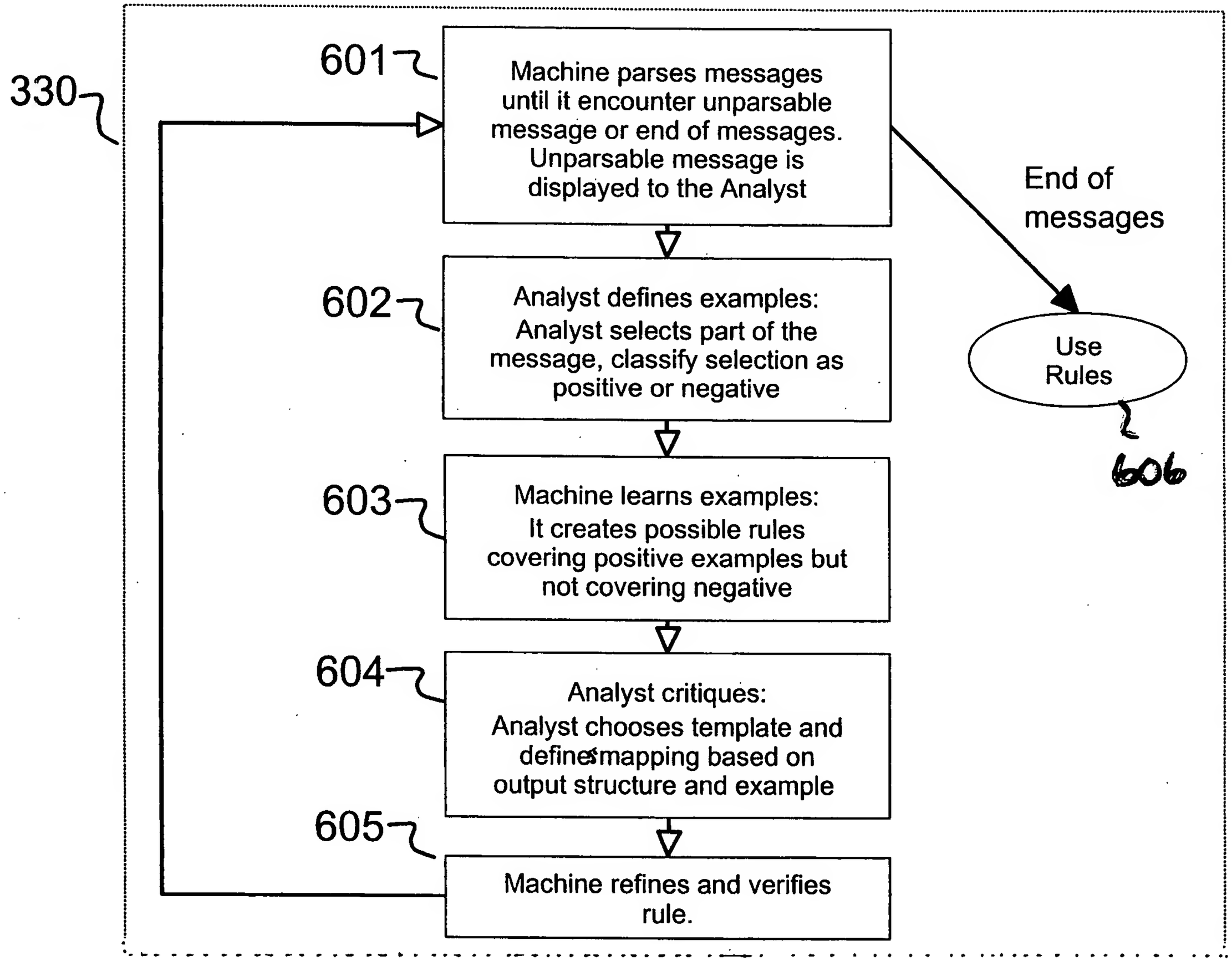

Machine builds message skeleton
501
Skeleton is matched against existing templates
502
Possible matches are provided to analyst to choose from
503
Sufficient message structure?
504
Yes
No
Use Message Structure
506
Analyst chooses part of the message, maps it to the message structure classifying as positive or negative
505
320

FIG.6



6/8
10829003032 US1

FIG. 7

700

```
<?xml version="1.0" encoding="UTF-8" ?>
<schema targetNamespace="http://OutputStructure.xsd">
        <element name="OutputStructure">
                <complexType>
                        <sequence>
                                <element ref="Fields" maxOccurs="unbounded" />
                        </sequence>
                        <attribute name="separator" use="required" type="string" />
                        <attribute name="hashing" use="optional" type="string" />
                </complexType>
        </element>
        <element name="Fields">
                <complexType>
                        <sequence>
                                <element ref="GroupsMsgDataElement" minOccurs="0" maxOccurs="1" />
                                <element ref="RuleAttCreationTime" />
                                <element ref="RuleAttSeverity" />
                        </sequence>
                        <attribute name="Match" type="string" />
                        <attribute name="Substitute" type="string" />
                        <attribute name="Split" type="string" />
                        <attribute name="Name" type="string" />
                        <attribute name="Description" type="string" />
                </complexType>
        </element>
        <element name="RuleAttCreationTime">
                <complexType>
                        <sequence>
                                <element ref="Subs" minOccurs="1" maxOccurs="unbounded" />
                        </sequence>
                        <attribute name="Value" type="string" use="optional"/>
                </complexType>
        </element>
        <element name="Subs">
                <complexType>
                        <attribute name="Positions" type="string" />
                        <attribute name="Match" type="string" />
                        <attribute name="Substitute" type="string" />
                        <attribute name="TimeFormat" type="string" />
                </complexType>
        </element>
</schema>
```

7/8
20120326051

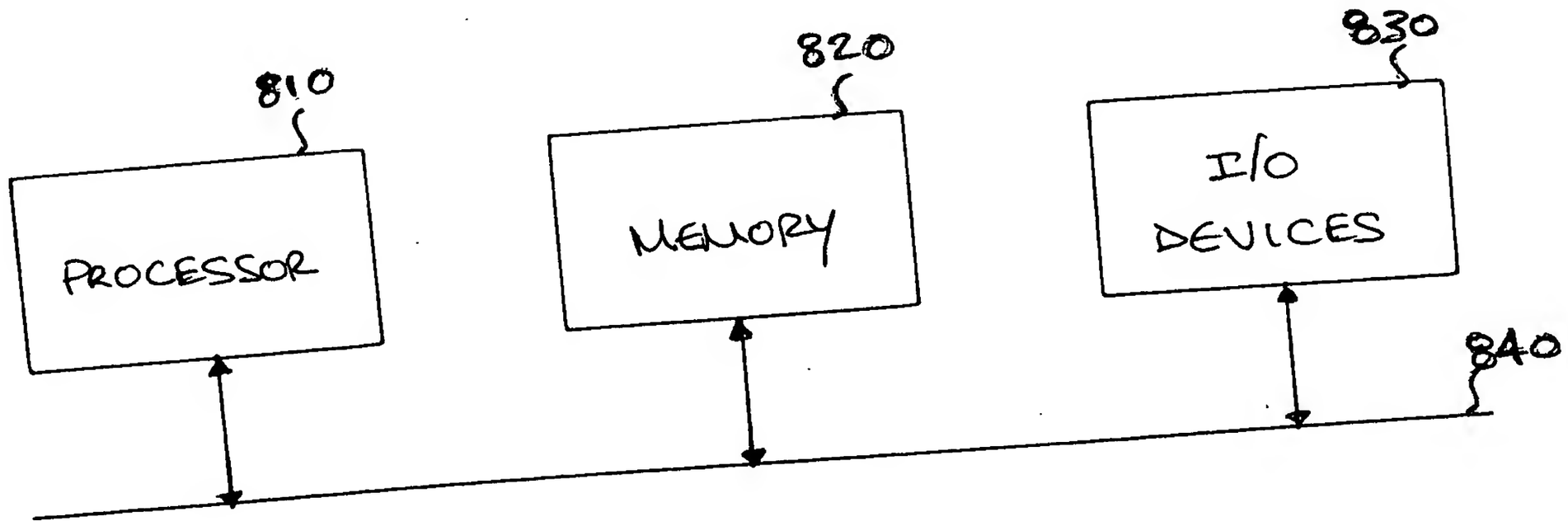


FIG. 8